DATA PROTECTION POLICY

INTRODUCTION

This Data Protection Policy defines how Harrow International School Bengaluru will meet its obligations with regards to personal data.

SCOPE

All employees, contractors, agents, consultants, partners or other members of the School who have access to any personal data held by or on behalf of the School, must comply with this Policy and any supporting policies, procedures and guidance in order to meet duties and responsibilities.

This policy should be read alongside any contract of employment (or contract for services) and any other notice we issue from time-to-time in relation to your data. This policy forms part of the terms and conditions of all employees' contracts of employment. A breach of the policy may be regarded as misconduct, leading to disciplinary action up to and including summary dismissal.

In order to operate safely and efficiently, the School has to collect and use personal data about people with whom it works ("data subjects") for the purposes set forth under this Policy and any supporting policies and procedures.

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials. The School may need to process special category personal data (concerning health, ethnicity, religious or philosophical beliefs, genetic or biometric data, sexual orientation) or criminal records information such as criminal convictions and offences in accordance with the rights and duties imposed on it, or from time to time by explicit consent where required or subject to the legal exemptions.

The School processes personal data:
• Where the data subject has given consent to the processing of his or her personal data for one or more specific purposes,
• Where processing is necessary for the performance of a contract (entering into employments contract, third party contracts etc.),
• Where processing is necessary for compliance with a legal obligation to which the School is subject (employment law requirements, assisting criminal investigations etc.),
• Where processing is necessary in order to protect the vital interests of the data subject or of another natural person (in situations where a data subject has a severe accident or illness at the School premises and needs immediate medical support),
• Where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the School,
• Where processing is necessary for the purposes of the legitimate interests the School (including but not restricted to: administering the School to the highest standards, providing the best education possible, increasing communications between the School, alumni and parents for fundraising purposes, and evaluation of employees' performances).

WORKING WITH SUPPLIERS, CONSULTANTS AND PARTNERS

In order to ensure the School meets its obligations to manage and protect personal data:
▪ due diligence must be undertaken on all suppliers, consultants and partners who will handle (process) personal data on behalf of the School, and
▪ any contract, processing or data sharing agreements signed between the School and a supplier, consultant and/or partner must contain the appropriate clauses.

HANDLING SUBJECT ACCESS REQUESTS (SARS) AND OTHER RIGHTS REQUESTS

Data subjects may:
▪ Request access to data about them held by the School;
▪ Prevent processing in certain circumstances such as for direct marketing purposes or where the processing relies on legitimate interests;
▪ Have inaccurate data about them amended;
▪ Request deletion of the data held by the School; and
▪ Object to data processing activities of the School that have disproportionate impact on their rights.

On receipt of a formal request, it should be immediately passed to the Head Master's EA. This will ensure that:
▪ the request can be processed in accordance with the appropriate procedure;
▪ the required checks and searches can be undertaken;
▪ if required, exemptions applied, and
▪ a compliant response can be provided.

ROUTINE DISCLOSURES AND USES OF PERSONAL DATA

School Departments may need to share and access personal data to provide services or deliver their functions. Also, the School may receive requests from third parties to disclose personal data it holds about data subjects.

The routine collection, use, disclosure and storage of personal data must be for legitimate purposes. For example, disclosures can occur in connection with:
▪ Safeguarding;
▪ The prevention or detection of crime;
▪ assessment or collection of any tax or duty;
▪ Where necessary to exercise a right or obligation conferred or imposed by law upon the School and
▪ References given by the School.

RECORDS RETENTION, DISPOSAL AND DATA ACCURACY

The School will endeavour to ensure that all personal data held in relation to data subjects is accurate. This applies to the data held for students and staff. The School makes clear that the burden of responsibility for accuracy of information held lies with the data subject e.g. it makes clear to parents that they must update the School about any changes to their child's personal data and asks the same of staff.

▪ Staff must notify the HR Department of any changes to personal data held about them.
▪ Staff must update personal data when they become aware it has become inaccurate.
▪ Parents & Pupils must notify the School of any changes to personal data by notifying the House Master or the Medical Centre, as appropriate.

DATA BREACH MANAGEMENT

All members of staff must immediately (as soon as they are aware) report any and all suspected or actual breaches to the Head Master, retaining any evidence in relation to the breach and sharing this forward as required.

Breaches should be reported as follows:
▪ IT-related – inform the IT service desk (who will the report to the Head Master)
▪ Non-IT related – inform your line manager (who will then report to the Head Master)

ENFORCEMENT
If an individual believes that the School has not complied with this Policy, he or she should notify the School's Privacy Officer. If an individual still has an issue, then they may use the School's Grievance or Complaints Procedure.

Policy Updated: July 2023
Review Date: July 2024